Configuração e recomendações do ASA NAT para a implementação das interfaces de rede duplas do Expressway-E

Contents

Introduction

Este documento descreve como implementar a configuração NAT (Network Address Translation) necessária no Cisco Adaptive Security Appliance (ASA) para a implementação de Interfaces de

Rede Duplas Expressway-E.

> **Dica**: essa implantação é a opção recomendada para a implementação do Expressway-E, em vez da implementação de NIC única com reflexão de NAT.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração básica do Cisco ASA e configuração de NAT
- Configuração básica do Cisco Expressway-E e Expressway-C

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Dispositivos Cisco ASA 5500 e 5500-X Series que executam o software versão 8.0 e posterior.
- Cisco Expressway versão X8.0 e posterior.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

> **Observação**: por meio de todo o documento, os dispositivos do expressway são chamados de Expressway-E e Expressway-C. No entanto, a mesma configuração se aplica aos dispositivos VCS (Video Communication Server, servidor de comunicação de vídeo) Expressway e VCS Control.

Informações de Apoio

O Cisco Expressway-E pode ser colocado em uma zona desmilitarizada (DMZ) ou em uma interface voltada para a Internet, enquanto pode se comunicar com o Cisco Expressway-C em uma rede privada. Quando o Cisco Expressway-E é colocado em uma DMZ, esses são os benefícios adicionais:

- No cenário mais comum, o Cisco Expressway-E é gerenciado pela rede privada. Quando o Cisco Expressway-E está em um DMZ, um firewall de perímetro (externo) pode ser usado para bloquear o acesso indesejado ao Expressway de redes externas através de solicitações HTTPS (Hypertext Transfer Protocol Secure) ou SSH (Secure Shell).
- Se a DMZ não permitir conexões diretas entre redes internas e externas, os servidores dedicados serão necessários para tratar o tráfego que atravessa a DMZ. O Cisco Expressway pode atuar como um servidor proxy para tráfego de voz e vídeo do Session Initiation Protocol (SIP) e/ou H.323. Nesse caso, você pode usar a opção Dual Network Interfaces (Interfaces

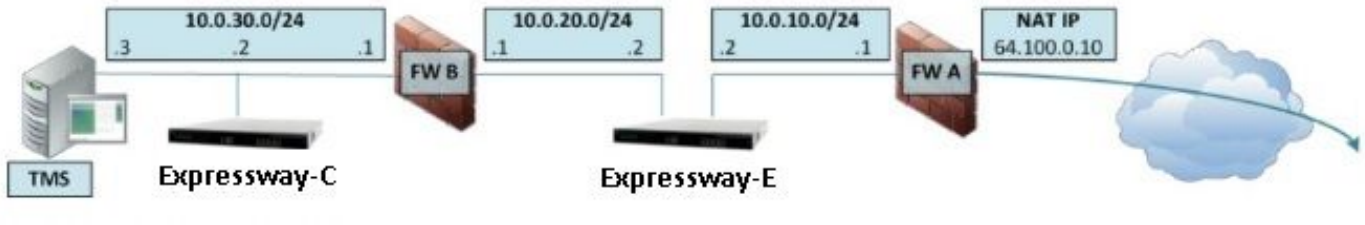
de rede duplas), que permite ao Cisco Expressway ter dois endereços IP diferentes, um para o tráfego de/para o firewall externo e outro para o tráfego de/para o firewall interno.

- Essa configuração evita conexões diretas da rede externa com a rede interna. Isso melhora a segurança da rede interna em geral.

Tip: Para obter mais detalhes sobre a implementação da TelePresence, consulte o Cisco Expressway-E e Expressway-C - Basic Configuration Deployment Guide e Colocando um Cisco VCS Expressway em uma DMZ em vez de na Internet pública.

Expressway C e E - duas interfaces de rede/implementação de NIC dupla

Esta imagem mostra um exemplo de implantação para um Expressway-E com interfaces de rede duplas e NAT estático. O Expressway-C atua como o cliente transversal. Há dois firewalls (FW A e FWB). Normalmente, nessa configuração de DMZ, o FW A não pode rotear o tráfego para o FW B, e dispositivos como o Expressway-E são necessários para validar e encaminhar o tráfego da sub-rede do FW A para a sub-rede do FW B (e vice-versa).



Essa implantação consiste nesses componentes.

Sub-rede DMZ 1 - 10.0.10.0/24

- FW Uma interface interna - 10.0.10.1
- Interface LAN2 Expressway-E - 10.0.10.2

Sub-rede DMZ 2 - 10.0.20.0/24

- Interface externa do firmware B - 10.0.20.1
- Interface LAN1 Expressway-E - 10.0.20.2

Sub-rede LAN - 10.0.30.0/24

- Interface interna do FW B - 10.0.30.1
- Interface LAN1 Expressway-C - 10.0.30.2
- Interface de rede do servidor Cisco TelePresence Management Suite (TMS) - 10.0.30.3

Especificações desta implementação:

- FW A é o firewall externo ou do perímetro; é configurado com NAT IP (IP público) de 64.100.0.10 que é estaticamente traduzido para 10.0.10.2 (interface LAN2 Expressway-E)
- FW B é o firewall interno
- A LAN1 Expressway-E tem o modo NAT estático desativado
- A LAN2 do Expressway-E tem o modo NAT estático ativado com o endereço NAT estático 64.100.0.10
- O Expressway-C tem uma zona cliente transversal que aponta para 10.0.20.2 (interface LAN1

Expressway-E)
- Não há roteamento entre as sub-redes 10.0.20.0/24 e 10.0.10.0/24. O Expressway-E liga essas sub-redes e atua como um proxy para a sinalização SIP/H.323 e para a mídia RTP (Real-time Transport Protocol) / RTCP (RTP Control Protocol).
- O Cisco TMS tem o Expressway-E configurado com o endereço IP 10.0.20.2

Requisitos/limitações

Sub-redes não sobrepostas

Se o Expressway-E estiver configurado para usar ambas as interfaces de LAN, as interfaces LAN1 e LAN2 devem estar localizadas em sub-redes não sobrepostas para garantir que o tráfego seja enviado para a interface correta.

Clustering

Ao agrupar dispositivos Expressway com a opção Advanced Networking configurada, cada peer de cluster precisa ser configurado com seu próprio endereço de interface LAN1. Além disso, o clustering deve ser configurado em uma interface que não tenha o modo NAT estático ativado. Portanto, é recomendável usar LAN2 como a interface externa, na qual você pode aplicar e configurar o NAT estático onde aplicável.

Configurações de interface LAN externa

As configurações da interface de LAN externa na página de configuração IP controlam qual interface de rede usa Transversal Usando Relés ao redor do NAT (TURN). Em uma configuração Expressway-E de interface de rede dupla, ela é normalmente definida para a interface LAN externa Expressway-E.

rotas estáticas

O Expressway-E deve ser configurado com um endereço de gateway padrão de 10.0.10.1 para esse cenário. Isso significa que todo o tráfego enviado via LAN2 é, por padrão, enviado ao endereço IP 10.0.10.1.

Se o FW B converte o tráfego enviado da sub-rede 10.0.30.0/24 para a interface LAN1 Expressway-E (por exemplo, tráfego de cliente transversal Expressway-C ou tráfego de gerenciamento de servidor TMS), esse tráfego aparece quando vem da interface externa FWB (10.0.20.1) enquanto alcança a LAN1 Expressway-E. O Expressway-E é então capaz de responder a esse tráfego através de sua interface LAN1, já que a fonte aparente desse tráfego está localizada na mesma sub-rede.

Se o NAT estiver ativado no FW B, o tráfego enviado do Expressway-C para a Expressway-E LAN1 mostrará como ele vem de 10.0.30.2. Se o Expressway não tiver uma rota estática adicionada para a sub-rede 10.0.30.0/24, ele enviará as respostas para esse tráfego para seu gateway padrão (10.0.10.1) de LAN2, pois não sabe que a sub-rede 10.0.30.0/24 está localizada atrás do firewall interno (FW B). Portanto, uma rota estática precisa ser adicionada, execute o comando **xCommand RouteAdd** CLI através de uma sessão SSH para Expressway.

Neste exemplo específico, o Expressway-E deve saber que pode acessar a sub-rede 10.0.30.0/24

atrás do FW B, que pode ser acessada através da interface LAN1. Para fazer isso, execute o comando:

```
xCommand RouteAdd Address: 10.0.30.0 PrefixLength: 24 Gateway: 10.0.20.1 Interface: LAN1
```

> **Nota**: Sa configuração de rota estática pode ser aplicada através da GUI do Expressway-E, bem como pela seção **System/Network > Interfaces/Static Routes**.

Neste exemplo, o parâmetro Interface também pode ser definido como **Automático** como o endereço de gateway (10.0.20.1) só pode ser alcançado via LAN1.

Se o NAT não estiver habilitado no FW B e o Expressway-E precisar se comunicar com dispositivos em sub-redes (diferentes de 10.0.30.0/24) que também estão localizadas atrás do FW B, as rotas estáticas deverão ser adicionadas para esses dispositivos/sub-redes.

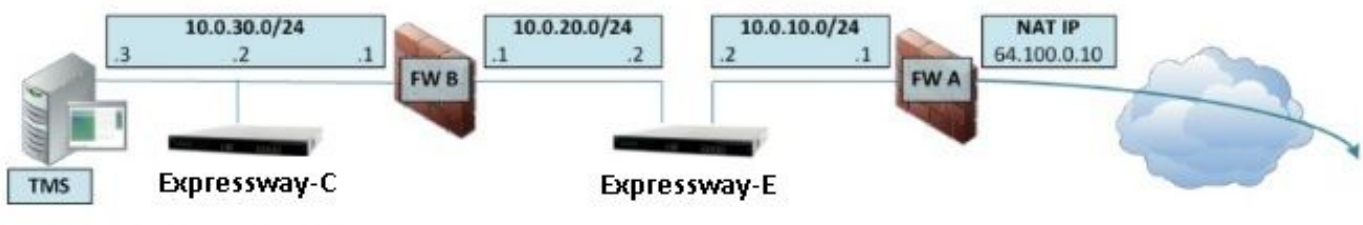
> **Note**: Isso inclui Conexões SSH e HTTPS de estações de trabalho de gerenciamento de rede ou para serviços de rede como NTP, DNS, LDAP/AD ou Syslog.

O comando e a sintaxe **xCommand RouteAdd** são descritos em detalhes completos no VCS Administrator Guide.

Configuração

Esta seção descreve como configurar o NAT estático necessário para a implementação da interface de rede dupla Expressway-E no ASA. Algumas recomendações adicionais de configuração do ASA Modular Policy Framework (MPF) estão incluídas para o tratamento do tráfego SIP/H323.

Expressway C e E - Interfaces de rede duplas/Implementação de NIC dupla



Neste exemplo, a atribuição de endereço IP é a próxima.

Endereço IP do Expressway-C: 10.0.30.2/24

Gateway padrão Expressway-C: 10.0.30.1 (FW-B)

Endereços IP do Expressway-E:

LAN2: 10.0.10.2/24

Na LAN1: 10.0.20.2/24

Gateway padrão Expressway-E: 10.0.10.1 (FW-A)

Endereço IP do TMS: 10.0.30.3/24

Configuração do FW-A

Etapa 1. Configuração de NAT estático para o Expressway-E.

Como explicado na seção Informações de Fundo deste documento, o FW-A tem uma tradução NAT estática para permitir que o Expressway-E seja acessível da Internet com o endereço IP público 64.100.0.10. Este último é NATed para o endereço IP 10.0.10.2/24 da LAN2 do Expressway-E. Dito isso, essa é a configuração de NAT estático do FW-A necessária.

Para as versões 8.3 e posterior do ASA:

```
! To use PAT with specific ports range:

object network obj-10.0.10.2
host 10.0.10.2

object service obj-udp_3478-3483 service udp source range 3478 3483 object service obj-
udp_24000-29999 service udp source range 24000 29999 object service obj-udp_36002-59999 service
udp source range 36002 59999 object service obj-tcp_5222 service tcp source eq 5222 object
service obj-tcp_8443 service tcp source eq 8443 object service obj-tcp_5061 service tcp source
eq 5061 object service obj-udp_5061 service udp source eq 5061 nat (inside,outside) source
static obj-10.0.10.2 interface service obj-udp_3478-3483 obj-udp_3478-3483 nat (inside,outside)
source static obj-10.0.10.2 interface service obj-udp_24000-29999 obj-udp_24000-29999 nat
(inside,outside) source static obj-10.0.10.2 interface service obj-udp_36002-59999 obj-
udp_36002-59999 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_5222
obj-tcp_5222 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_8443
obj-tcp_8443 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_5061
obj-tcp_5061 nat (inside,outside) source static obj-10.0.10.2 interface service obj-udp_5061
obj-udp_5061 OR ! To use with static one-to-one NAT: object network obj-10.0.10.2 nat
(inside,outside) static interface
```

> **Cuidado**: ao aplicar os comandos PAT estáticos, você recebe esta mensagem de erro na interface de linha de comando do ASA, "**ERRO: O NAT não pode reservar portas"**. Depois disso, prossiga para limpar as entradas xlate no ASA, para isso, execute o comando **clearxlatelocal x.x.x.x,** de onde x.x.x.x corresponde ao endereço IP externo do ASA. Esse comando limpa todas as conversões associadas a esse endereço IP, executa-o com cuidado em ambientes de produção.

Para as versões 8.2 e anterior do ASA:

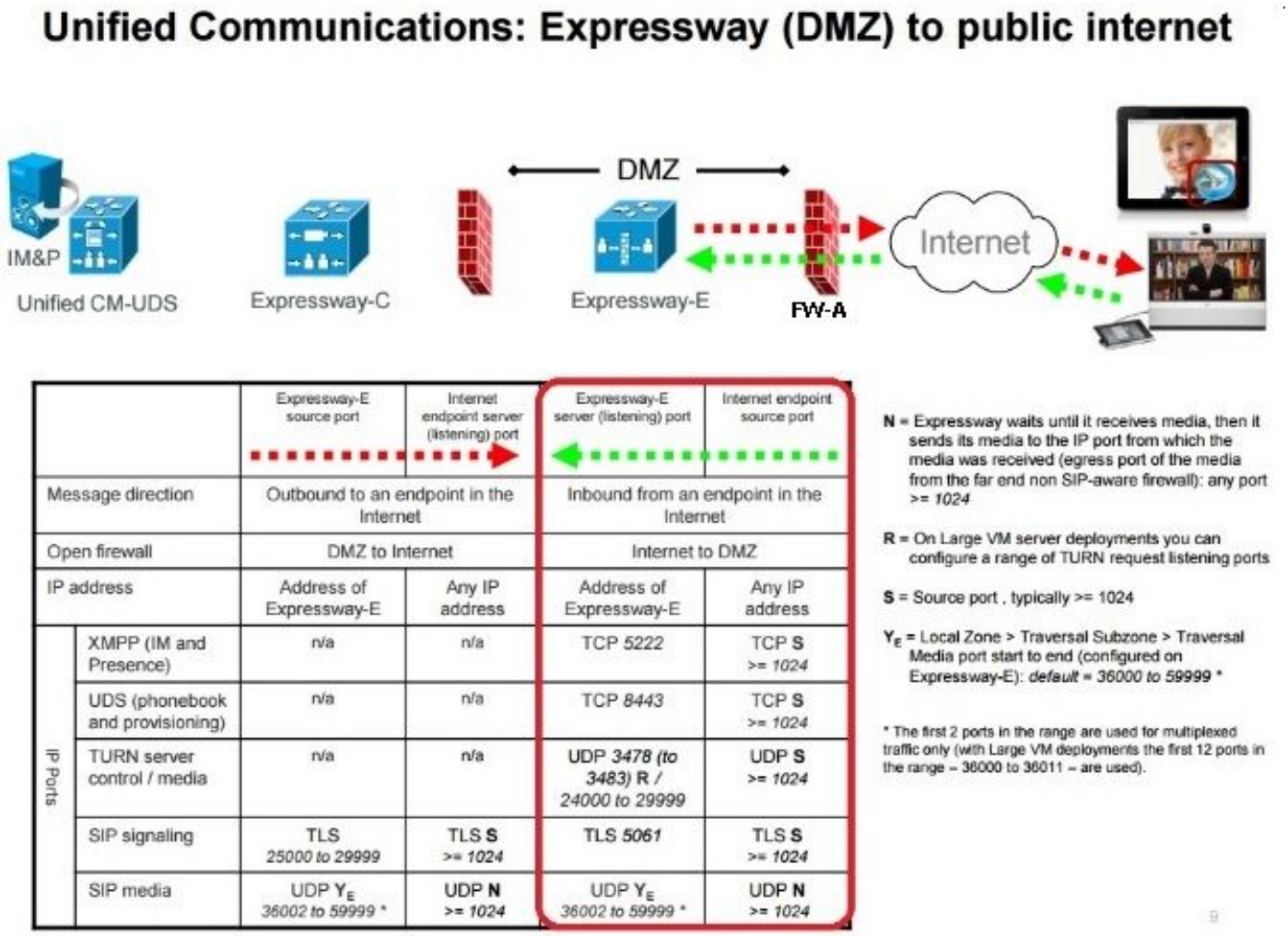
```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Etapa 2. A configuração da ACL (Access Control List, lista de controle de acesso) permite as portas necessárias da Internet para o Expressway-E.

De acordo com a Comunicação Unificada: O Expressway (DMZ) para a documentação da Internet pública, a lista de portas TCP e UDP que o Expressway-E exige para permitir no FW-A, são como

mostrado na imagem:



		Expressway-E source port	Internet endpoint server (listening) port	Expressway-E server (listening) port	Internet endpoint source port
Message direction		Outbound to an endpoint in the Internet		Inbound from an endpoint in the Internet	
Open firewall		DMZ to Internet		Internet to DMZ	
IP address		Address of Expressway-E	Any IP address	Address of Expressway-E	Any IP address
IP Ports	XMPP (IM and Presence)	n/a	n/a	TCP *5222*	TCP **S** *>= 1024*
	UDS (phonebook and provisioning)	n/a	n/a	TCP *8443*	TCP **S** *>= 1024*
	TURN server control / media	n/a	n/a	UDP *3478 (to 3483)* **R** / *24000 to 29999*	UDP **S** *>= 1024*
	SIP signaling	TLS *25000 to 29999*	TLS **S** *>= 1024*	TLS *5061*	TLS **S** *>= 1024*
	SIP media	UDP Y_E *36002 to 59999 **	UDP **N** *>= 1024*	UDP Y_E *36002 to 59999 **	UDP **N** *>= 1024*

N = Expressway waits until it receives media, then it sends its media to the IP port from which the media was received (egress port of the media from the far end non SIP-aware firewall): any port *>= 1024*

R = On Large VM server deployments you can configure a range of TURN request listening ports

S = Source port , typically >= 1024

Y_E = Local Zone > Traversal Subzone > Traversal Media port start to end (configured on Expressway-E): *default = 36000 to 59999* *

* The first 2 ports in the range are used for multiplexed traffic only (with Large VM deployments the first 12 ports in the range – 36000 to 36011 – are used).

Essa é a configuração da ACL necessária como entrada na interface externa do FW-A.

Para as versões 8.3 e posterior do ASA:

```
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5222
access-list outside-in extended permit tcp any host 10.0.10.2 eq 8443
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
access-list outside-in extended permit udp any host 10.0.10.2 lt 3484
access-list outside-in extended permit udp any host 10.0.10.2 gt 23999
access-list outside-in extended permit udp any host 10.0.10.2 lt 30000
access-list outside-in extended permit udp any host 10.0.10.2 gt 36001
access-list outside-in extended permit udp any host 10.0.10.2 lt 60000
access-list outside-in extended permit udp any host 10.0.10.2 eq 5061
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5061

access-group outside-in in interface outside
```

Para as versões 8.2 e anterior do ASA:

```
access-list outside-in extended permit tcp any host 64.100.0.10 eq 5222
access-list outside-in extended permit tcp any host 64.100.0.10 eq 8443
access-list outside-in extended permit udp any host 64.100.0.10 gt 3477
access-list outside-in extended permit udp any host 64.100.0.10 lt 3484
access-list outside-in extended permit udp any host 64.100.0.10 gt 23999
access-list outside-in extended permit udp any host 64.100.0.10 lt 30000
```

```
access-list outside-in extended permit udp any host 64.100.0.10 gt 36001
access-list outside-in extended permit udp any host 64.100.0.10 lt 60000
access-list outside-in extended permit udp any host 64.100.0.10 eq 5061
access-list outside-in extended permit tcp any host 64.100.0.10 eq 5061

access-group outside-in in interface outside
```

Configuração do FW-B

Conforme explicado na seção Informações de Fundo deste documento, o FW B pode exigir uma configuração NAT ou PAT dinâmica para permitir que a sub-rede interna 10.0.30.0/24 seja convertida para o endereço IP 10.0.20.1 quando for para a interface externa do FW B.

Para as versões 8.3 e posterior do ASA:

```
object network obj-10.0.30.0
   subnet 10.0.30.0 255.255.255.0
   nat (inside,outside) dynamic interface
```

Para as versões 8.2 e anterior do ASA:

```
nat (inside) 1 10.0.30.0 255.255.255.0
global (outside) 1 interface
```

> **Dica**: certifique-se de que todas as portas TCP e UDP necessárias permitem que o Expressway-C funcione corretamente e estejam abertas no FW B, conforme especificado neste documento da Cisco: Uso da porta IP do Cisco Expressway para passagem de firewall

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

O Packet Tracer pode ser usado no ASA para confirmar se a tradução NAT estática Expressway-E funciona conforme necessário.

Packet Tracer para testar 64.100.0.10 no TCP/5222

```
FW-A#packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 5222

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/5222 to 10.0.10.2/5222

Phase: 2
Type: ACCESS-LIST
Subtype: log
```

```
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5222
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 13, packet dispatched to next module

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow
```

Packet Tracer para testar 64.100.0.10 no TCP/8443

```
FW-A# packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 8443

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/8443 to 10.0.10.2/8443

Phase: 2
Type: ACCESS-LIST
```

```
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 10.0.10.2 eq 8443
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 14, packet dispatched to next module

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow
```

Packet Tracer para testar 64.100.0.10 no TCP/5061

```
FW-1# packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 5061

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/5061 to 10.0.10.2/5061

Phase: 2
```

```
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5061
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 15, packet dispatched to next module

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow
```

Packet Tracer para testar 64.100.0.10 em UDP/24000

```
ASA1# packet-tracer input outside udp 4.2.2.2 1234 64.100.0.10 24000

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/24000 to 10.0.10.2/24000
```

```
Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 16, packet dispatched to next module

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow
```

Packet Tracer para o teste 64.100.0.10 em UDP/36002

```
ASA1# packet-tracer input outside udp 4.2.2.2 1234 64.100.0.10 36002

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/36002 to 10.0.10.2/36002
```

```
Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 17, packet dispatched to next module

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow
```

Troubleshoot

Etapa 1. Comparar Capturas de Pacotes.

As capturas de pacotes podem ser feitas nas interfaces de entrada e saída do ASA.

```
FW-A# sh cap
capture capout interface outside match ip host 64.100.0.100 host 64.100.0.10
```

```
capture capin interface inside match ip host 64.100.0.100 host 10.0.10.2
```

Capturas de pacotes para 64.100.0.10 no TCP/5222:

```
FW-A# sh cap capout

2 packets captured
   1: 21:39:33.646954 64.100.0.100.21144 > 64.100.0.10.5222: S 4178032747:4178032747(0) win 4128
<mss 1460>
   2: 21:39:35.577652 64.100.0.100.21144 > 64.100.0.10.5222: S 4178032747:4178032747(0) win 4128
<mss 1460>
2 packets shown

FW-A# sh cap capin

2 packets captured
   1: 21:39:33.647290 64.100.0.100.21144 > 10.0.10.2.5222: S 646610520:646610520(0) win 4128
<mss 1380>
   2: 21:39:35.577683 64.100.0.100.21144 > 10.0.10.2.5222: S 646610520:646610520(0) win 4128
<mss 1380>
2 packets shown
```

Capturas de pacotes para 64.100.0.10 no TCP/5061:

```
FW-A# sh cap capout
2 packets captured

   1: 21:42:14.920576 64.100.0.100.50820 > 64.100.0.10.5061: S 2023539318:2023539318(0) win 4128
<mss 1460>
   2: 21:42:16.992380 64.100.0.100.50820 > 64.100.0.10.5061: S 2023539318:2023539318(0) win 4128
<mss 1460>
2 packets shown
FW-A# sh cap capin 2 packets captured 1: 21:42:14.920866 64.100.0.100.50820 > 10.0.10.2.5061: S
2082904361:2082904361(0) win 4128 <mss 1380> 2: 21:42:16.992410 64.100.0.100.50820 >
10.0.10.2.5061: S 2082904361:2082904361(0) win 4128 <mss 1380> 2 packets shown
```

Etapa 2. Inspecione Capturas de Pacotes de Descarte do ASP (Accelerated Security Path, Caminho de Segurança Acelerado).

As quedas de pacotes por um ASA são capturadas pela captura do ASA ASP. A opção **all**, captura todos os possíveis motivos pelos quais o ASA descartou um pacote. Isso pode ser reduzido se houver alguma razão suspeita. Por uma lista de motivos que um ASA usa para classificar essas quedas, execute o comando **show asp drop.**

```
capture asp type asp-drop all

show cap asp

OR

show cap asp | i 64.100.0.10
show cap asp | i 10.0.10.2
```

> **Tip**: A captura ASA ASP é usada neste cenário para confirmar se o ASA descarta pacotes devido a uma configuração de ACL ou NAT perdida, que exigiria abrir uma porta TCP ou UDP específica para o Expressway-E.

> **Tip**: O tamanho de buffer padrão para cada captura ASA é de 512 KB. Se muitos pacotes

forem descartados pelo ASA, o buffer será preenchido rapidamente. O tamanho do buffer pode ser aumentado com a opção **buffer**.

Recomendações

Verifique se a inspeção SIP/H.323 está completamente desabilitada nos firewalls envolvidos.

Éaltamente recomendado desativar a inspeção SIP e H.323 em firewalls que tratam do tráfego de rede de ou para um Expressway-E. Quando ativada, a inspeção de SIP/H.323 frequentemente afeta negativamente a funcionalidade de passagem de firewall/NAT incorporada do Expressway.

Este é um exemplo de como desativar as inspeções SIP e H.323 no ASA:

```
policy-map global_policy
 class inspection_default
  no inspect h323 h225
  no inspect h323 ras
  no inspect sip
```

Implementação alternativa do VCS Expressway

Uma solução alternativa para implementar o Expressway-E com interface de rede dupla/NIC dupla é implementar o Expressway-E, mas com uma única placa de rede e configuração de reflexão NAT nos firewalls. O link a seguir mostra mais detalhes sobre essa implementação Configurar reflexão de NAT no ASA para dispositivos de telepresença do VCS Expressway.

> **Tip**: A implementação recomendada para o VCS Expressway é a implementação de interfaces de rede duplas/NIC VCS Expressway dupla descrita neste documento.

Informações Relacionadas

- Configure a reflexão de NAT no ASA para dispositivos de telepresença do VCS Expressway
- Suporte Técnico e Documentação - Cisco Systems
- Cisco Expressway-E e Expressway-C - Guia de implantação de configuração básica
- Como colocar um Cisco VCS Expressway em uma DMZ em vez de na Internet pública
- Uso da porta IP do Cisco Expressway para passagem de firewall